REMARKS

Claims 1-13, 16-21, 24-34, 36 and 38-41 are currently pending in the subject application, and are presently under consideration. Claims 1-13, 16-21, 24-34, 36 and 38-41 are rejected. Favorable reconsideration of the application is requested in view of the amendments and comments herein.

I. Rejection of Claims 1-13 and 16-19 Under 35 U.S.C. §103(a)

Claims 1-13 and 16-19 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Funk, U.S. Patent No. 5,721,779 ("Funk") in view of Keene, et al., U.S. Publication No. 2004/0049294 ("Keene") in further view of Carter, U.S. Patent No. 6,760,843 ("Carter"). Claim 1 has been amended to clarify the phrase "filtering and displaying messages broadcast or multicast within the network." Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claim 1, as amended, recites a method of administering access and security on a network having a plurality of computers. A one-way encrypted password file is installed on each computer of the plurality of computers in the network. The one-way encrypted password file includes a plurality of user identifications associated one-way encrypted passwords and associated privileges for each authorized user allowed access to the plurality of computers and the network. A password entered by a user is one-way encrypted when the user logs into a computer of the plurality of computers on the network. A match is checked for between the user identification and one-way encrypted password entered by the user and the plurality of user identifications and one-way encrypted passwords stored in the one-way encrypted password file. Access is enabled to data and software contained on the computer and the network permitted by the associated privileges for the user when a match is found on the one-way encrypted password file. Messages are broadcast to the plurality of computers, such that each message is received at each computer. The broadcast messages are filtered at each computer according to the associated privileges of the user associated with each computer, such that a given message will

be displayed only where the associated privileges of the user allow the message to be displayed. The one way encrypted password file at each of the plurality of computers is updated by attaching a new master password file to a message at a computer accessible by a systems administrator or security officer, encrypting the message containing the new master password file using a private key and pass phrase available only to the systems administrator or security officer, transmitting the message to the plurality of computers, and decrypting the message at each computer using a public key corresponding to the private key.

Neither Funk nor Keene teaches broadcasting messages to a plurality of computers and filtering the broadcast messages at each computer. The Office Action notes that Funk does not teach this element, but cites paragraph 0007 of the Keene patent as providing a teaching of broadcasting and filtering messages. The cited paragraph reads as follows:

> In operation, after given [sic]an access identification, a user can access *the database system* and request access to an object. The *system then retrieves* information pertaining to the individual user's privilege criteria and determines which information contained in the database may be accessed by the requestor. The *system then filters* the information including objects, their attributes and associated documents according to the privilege information and gives the user limited access to the information. The *requested and approved information can then be sent to the requestor of the information.* This could also be displayed to the user as a document file having a redacted document, blocking out the information that the user is not privileged to see. (Keene, ¶0007, emphasis added)

The Keene publication teaches a method for restricting access to data on a host computer. Each individual or organization that may have an interest in the data can access the host computer according to a password, with a given password granting access to certain categories of data. As is referenced in the Office Action, the Keene reference is capable of retrieving redacted portions of documents from a central server and displaying them to a requesting user. But as this passage makes clear, all of this filtering occurs at the database itself, so there is no teaching or suggestion of broadcasting a plurality of messages to a plurality of computers and filtering the broadcast messages in the Keene system, as recited in claim 1. Carter does not remedy this deficiency. It is thus respectfully submitted that claim 1 is patentable over the cited art.

Turning to the claims depending from claim 1, the applicant asserts that each dependent claim has its own specific limitations and features that define patentable invention over the prior art. For the sake of brevity, the discussion of certain dependent claims will be omitted. In focusing the discussion on specific claims, a concession of the patentable distinctiveness of the others is not intended.

Claim 5, which depends from claim 3, recites spoofing the user into believing that access has been gained to the computer upon request of the systems administrator or security officer, wherein spoofing includes the presentation of false messages and information to the user.

Neither of the cited references discuss providing an unauthenticated user with false data in any form. The Office Action cites the following portion of Funk:

> As further illustrated by FIG. 2, the processor element 16 connects via a transmission path to the communication port 18. The communication port 18 can be an electrical circuit card assembly of the type conventionally used for interfacing a computer element with a communication channel, such as the communication channel 22. In one embodiment of the present invention the communication port 18 includes a modem for transforming electrical digital data signals into a format suitable for transmission over conventional telephone wires. Alternatively the communication port 18 can be a hard wired parallel computer interface of the type suitable for connecting a computer processing element such as host element 44 with a terminal interface such as the type as used by an ATM device. In the illustrated embodiment, the processing element 16 can include a second operating program stored in the program memory for directing the processing unit to operate the communication port 18 to transmit the challenge signal 26 via the communication channel 22 to the client element 46. The transmission of the challenge signal 26 can be responsive to an access request signal generated by the client element 46 and transmitted via the communication channel 22 and the communication port 18 to the processing element 16. However, it should be apparent to one of ordinary skill in the art, that other protocols and systems can be used for activating the transmission of the challenge signal 26 by the host element 44.
>
> The host element 44 further includes a comparator element 24. The comparator element 24 can be an electrical circuit card assembly constructed according to well known principles of electrical engineering, for comparing two large digital data signals and for determining a substantial identity between the two compared signals. In the illustrated embodiment, the comparator element 24 connects via transmission paths to the processor element 16 and the

> communication port 18. As further illustrated by FIG. 2, the comparator element 24 can further connect to the optional controller unit 42.
>
> The comparator element 24 can receive the key signal 30 generated by the processor element 16 and the response signal 28 received at the communication port 18 via the communication channel 22. The comparator element 24 compares the response signal 28 with the key signal 30 and generates a match signal 34 representative of a substantial identity between the response signal 28 and the key signal 30. (Funk, Col. 12, lines 20-64).

The cited paragraph describes the processing of the challenge signal at a processor associated with a central database, but there is no discussion of anything more than refusing to accept an incorrect password. The only data generated in the paragraph is the key, which is neither provided to the user nor misleading. The idea of providing false information to mislead an unauthenticated user is not suggested by this passage or any other portion of Funk. Keene and Carter also fail to teach or suggest spoofing a user attempting to access the system. Accordingly, it is respectfully submitted that claim 5 is nonobvious and patentable over the cited art.

Claim 6, which depends from claim 3, recites disabling a computer system to prevent access by the user upon a request by the system administrator. Funk, Keene and Carter, taken alone or in combination, fail to teach or suggest disabling a system upon one or more rejections of user provided authentication. As discussed above, Funk, Keene, and Carter simply provide for the rejection incorrect passwords and do not teach or suggest further action in response to multiple failed log-on attempts. The Office Action cites the following passage from Funk in rejecting claim 6:

> In a further alternative embodiment, the system 10 can include a processor 16 and a processor 20 that are adapted to implement a second randomizing operation that can add further security to the public communication channel. This second randomizing operation can include a response signal digest operation, such as an MD5 operation, that encrypts the response signal 28 to generate an encrypted response signal for transmission over a public communication channel. The server employs the same digest operation to encrypt the key signal 30 to generate an encrypted key signal and the comparator 24 compares these doubly encrypted signals. Both the client and the server can retain or exchange any common encryption keys or other data necessary for the selected digest operation.

> A match indicates that the client has met the server's challenge and the system 10 grants access to the client. (Funk, Col. 8, lines 47-63).

This passage simply describes a randomization process for the encryption keys used in the authentication process. There is no teaching of disabling a computer system in response to a request from a system administrator. Accordingly, it is respectfully submitted that claim 6 is nonobvious and patentable over the cited combination of Funk, Keene, and Carter.

Claim 7, which depends from claim 6, recites deleting a plurality of files from the computer system upon a request by the systems administrator or security officer. None of the cited references discusses remotely deleting system files to prevent an unauthorized user from accessing them. The Office Action cites a passage within Funk, discussing the encrypted challenge and response process used in authenticating in a user. It is thus respectfully submitted that claim 7 is nonobvious and patentable over the cited art.

Claim 8, which depends from claim 1, recites displaying a request for reauthentication at the direction of a system administrator or security officer. Claim 9, which depends from claim 8, requires that this reauthentication will take the form of a displayed log-in screen having a position for entry of the user identification and password. The Office Action cites two passages in Funk describing an initial authentication procedure. The claims, however, recite a reauthentication process, requiring an already authenticated user to reenter a user identification and password just to maintain the present connection upon the request of a system administrator. Neither of the cited references discusses such a reauthentication process. It is thus respectfully submitted that claims 8 and 9 are nonobvious and patentable over the cited references.

Dependent claims 2-13 and 16-19 depend directly or indirectly from independent claim 1. The applicant asserts that these claims are nonobvious and patentable for the reasons discussed above under claim 1 and for their own unique elements.

For the reasons described above, claims 1-13 and 16-19 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

II. Rejection of Claims 20-13 and 16-19 Under 35 U.S.C. §103(a)

Claims 20, 21, 24-34, 36 and 38-41 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Funk in view of Keene in further view of Jones, U.S. Patent No. 5,289,540 ("Jones"). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claim 20 recites a system to administer access and security on a network having a plurality of computers. The system includes a one-way encrypted password file on each computer of the plurality of computers in the network. The one-way encrypted password files include a plurality of user identifications, associated one-way encrypted passwords, and associated privileges for each authorized user allowed access to the plurality of computers and the network. A user login module receives a user identification or role and password from a user and logs in the user when a match is found in the one-way encrypted password file. A channel monitoring and filtering module monitors and receives broadcast or multicast messages within the network and displays the message to the user when the user's associated privileges permit the viewing of the message. A remote auditing module is operative to monitor and process anomalous events which may occur on the computer. The anomalous events comprise a change in the users' associated privileges, a system disable operation initiated by the user, the expiration of a user's password, the rejection of a message due to an invalid digital signature, a request for remote user re-authentication received from the systems administrator or security officer, a request for a remote user lockout received from the system administrator or security officer, and successful completion of a request for remote loading passwords to a system administrator or security officer.

None of the cited art teaches or suggests the filtering and display of broadcast or multicast messages based upon user privileges, either alone or in combination. The Office Action notes that Funk does not teach this element, but cites a portion of the Keene patent as providing the required teaching. The Keene publication teaches a method for restricting access to data on a host computer. Each individual or organization that may have an interest in the data

can access the host computer according to a password, with a given password granting access to certain categories of data. The cited paragraph (0007) merely describes this function.

The Examiner points out that the Keene system provides a privilege application 408 for documents retrieved from an application database 144 at an information retention system 138, such that access to documents can be refused or portions of the document can be redacted according to the requesting user's level of privilege. The data filtered by the Keene system consists solely of objects stored in the database, however, and does not include multicast or broadcast messages, as recited in claim 20. The information is retrieved from the database 144 in the information retention system 138, filtered at the privilege application 408 at the information retention system, and sent to the requesting user at a guest or host terminal. (*See* Keene, Fig. 1 and Fig. 8 and accompanying text). The data in the Keene system is both retrieved and filtered at the information retention system 138; it is not sent anywhere over the network prior to filtering. Thus, the data that is filtered in Keene is not in any way multicast or broadcast.

To monitor, receive, and selectively display multicast messages, a system would require structures at various points in the system to perform these functions. The system of claim 20 includes a channel monitoring and filtering module at each computer in the network that performs this function. The Keene system does not contain the distributed filtering that would be required for the filtering of multicast and broadcast messages. The guest database privilege application (170) at each of the guest computers of Keene simply confirms the password of a given user and provides the confirmed user identity to the host computer along with a data request (*See* Keene, ¶ 0040). There is no filtering of data at the guest privilege application. Jones also fail to teach or suggest the filtering of multicast or broadcast messages. If the Examiner persists in this rejection, it is respectfully requested that the Examiner provide a specific teaching or suggestion in Keene of the filtering of multicast or broadcast messages.

The cited art also fails to teach or suggest a remote auditing module operative to monitor and process anomalous events, including a change in a users' associated privileges, a system disable operation initiated by the user, the expiration of a user's password, the rejection of a

message due to an invalid digital signature, a request for remote user re-authentication received from the systems administrator or security officer, a request for a remote user lockout received from the system administrator or security officer, and successful completion of a request for remote loading passwords to a system administrator or security officer. The Examiner admits that neither Funk nor Keene provide such a teaching, but cites a file security system in Jones as providing a teaching of the remote auditing module. It is respectfully submitted that the file security system of Jones does not teach or suggest the cited module.

The file system of Jones monitors a computer system for a number of events, including corruption in key processes and files on a computer and repeated, unsuccessful attempts to log on to the system (*See* Fig. 4). Jones does not teach or suggest a module that is operative to monitor for even one of the events recited in claim 20. The Office Action cites Fig. 4 and its related text as providing this teaching, but the cited figure illustrates only the monitoring of unsuccessful user log in attempts, and there is no related text directly associated with the figure that might serve to provide additional teachings. (*See* Jones, Col. 10, lines 62-63). Accordingly, it is respectfully submitted that Jones does not teach the cited module and that claim 20 is patentable over the cited art.

Claim 31 recites a computer program executable by a computer and embedded in a computer readable medium to administer access and security on a network having a plurality of computers. A one-way encrypted password file is provided on each computer of the plurality of computers in the network. The one-way encrypted password file includes a plurality of user identifications, associated one-way encrypted passwords, and associated privileges for each authorized user allowed access to the plurality of computers and the network. A user login code segment receives a user identification or role and password from a user and logs in the user when a match is found in the one-way encrypted password file. A channel monitoring and filtering code segment monitors and receives broadcast or multicast messages within the network and displays the message to the user when the user's associated privileges permit the viewing of the message. A remote control code segment enables a system administrator or security officer to take appropriate action when an anomalous event transpires. The appropriate actions include the

act of spoofing the user into believing that the access has been gained to the computer, wherein spoofing includes the presentation of false messages and information to the user.

As discussed above under claim 20, the cited art does not teach or suggest the filtering and display of broadcast or multicast messages based upon user privileges, taken alone or in combination. In addition, the cited art does not teach or suggest a remote control code segment operative to allow a system administrator or security officer to spoof a user into believing that access has been gained to the computer, wherein spoofing includes the presentation of false messages and information to the user. None of the cited references discuss providing an unauthenticated user with false data in any form. The Office Action cites a portion of Funk describing the processing of the challenge signal at a processor associated with a central database, but there is no discussion of anything more than refusing to accept an incorrect password. Neither Jones nor Keene remedies this deficiency. The idea of providing false information to mislead an unauthenticated user is not suggested by this passage or any other portion of Funk. Accordingly, it is respectfully submitted that claim 31 is nonobvious and patentable over the cited art

Turning to the claims depending from claims 20 and 31, the applicant asserts that each dependent claim has its own specific limitations and features that define patentable invention over the prior art. For the sake of brevity, the discussion of certain dependent claims will be omitted. In focusing the discussion on specific claims, a concession of the patentable distinctiveness of the others is not intended.

Claims 25 and 36, which depend from claims 24 and 31 respectively, recite, when read in the context of the claims from which they depend, a remote control module operative to allow a system administrator or security officer to disable the computer system so that the user cannot access the computer system and delete a plurality of files stored in the computer in response to an anomalous event. None of the cited art teaches or suggests deleting a plurality of files from a system in response to an anomalous event. The Office Action cites a passage within the Funk, discussing the encrypted challenge and response process used in authenticating in a user. There is nothing in the cited passage that teaches the deletion of system files in response to an

anomalous event. Neither Keene nor Jones remedy this deficiency. It is thus respectfully submitted that claims 25 and 36 are nonobvious and patentable over the cited art.

Claim 26, which depends from claim 24, recites, when read in the context of the claim from which it depends, a remote control module operative to allow a system administrator or security officer to spoof a user into believing that access has been gained to the computer, wherein spoofing includes the presentation of false messages and information to the user. None of the cited references discuss providing an unauthenticated user with false data in any form. The Office Action cites a portion of Funk describing the processing of the challenge signal at a processor associated with a central database, but there is no discussion of anything more than refusing to accept an incorrect password. Neither Jones nor Keene remedies this deficiency. The idea of providing false information to mislead an unauthenticated user is not suggested by this passage or any other portion of Funk. Accordingly, it is respectfully submitted that claim 26 is nonobvious and patentable over the cited art.

Claim 34, which depends from claim 33, recites, when read in the context of the claim from which it depends, a remote auditing module operative to monitor and process anomalous events, including a change in a users' associated privileges, a system disable operation initiated by the user, the expiration of a user's password, the rejection of a message due to an invalid digital signature, a request for remote user re-authentication received from the systems administrator or security officer, a request for a remote user lockout received from the system administrator or security officer, and successful completion of a request for remote loading passwords to a system administrator or security officer. In the stated reasons for rejection of claim 20, the Examiner admits that neither Funk nor Keene, taken alone or in combination, provide such a teaching, but cites a passage in Funk in rejecting claim 34. (See Office Action of July 05, 2005, pg. 10, lines 10-18). The withdrawal of this rejection is respectfully requested as Funk, by the Examiner's own admission, does not contain the stated teaching. Further, it is respectfully submitted that Jones does not teach or suggest the cited code segment, for the reasons discussed above under claim 20. Accordingly, claim 20 is nonobvious over the cited art.

Claims 28 and 39, which depend from claims 20 and 31, respectively, recite displaying a request for reauthentication at the direction of a system administrator or security officer. The Office Action cites two passages in Funk describing an initial authentication procedure. The claims, however, discuss reauthentication, requiring an already authenticated user to reenter a user identification and password just to maintain the present connection upon the request of a system administrator. Neither Keene nor Jones remedy this deficiency. It is thus respectfully submitted that claims 28 and 39 are nonobvious and patentable over the cited references.

For the reasons described above, claims 20, 21, 24-34, 36 and 38-41 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

CONCLUSION

In view of the foregoing remarks, Applicant respectfully submits that the present application is in condition for allowance. Applicant respectfully requests reconsideration of this application and that the application be passed to issue.

Please charge any deficiency or credit any overpayment in the fees for this amendment to our Deposit Account No. 20-0090.

Respectfully submitted,

Date 9/20/05

Christopher P. Harris
Registration No. 43,660

CUSTOMER NO.: 26,294

TAROLLI, SUNDHEIM, COVELL, & TUMMINO L.L.P.
526 SUPERIOR AVENUE, SUITE 1111
CLEVELAND, OHIO 44114-1400
Phone: (216) 621-2234
Fax: (216) 621-4072